UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,906	12/28/2001	Nicholas Paul Kelly	01.103.01	2851

7590 09/12/2005

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

EXAMINER	
ALOMARI, FIRAS B	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 09/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/028,906	**Applicant(s)** KELLY ET AL.
	Examiner Firas Alomari	**Art Unit** 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 December 2001*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *06/05/2002*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-2, 7-12, 14-15, 20-25, 27-28 & 33-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chess et al. US (6,711,583) in view of Smithson et al. US (6,886,099).

Regarding claims 1, 14 & 27: A computer program product for operating a computer to review files for potential malware (Col 4, lines 4-10), comprising:

logging code operable to maintain a statistical log having an entry for each file sent to the computer for review, each entry being arranged to store a count value indicating the number of times that the file has been sent to the computer for review and a value of one or more predetermined attributes relating to the file (Col 4, line 62 through Col 5, line 5/ maintaining in the database the Nth occurrence of the document being scanned); statistical log interface code operable, upon receipt of a file, to determine with reference to the statistical log the count value relating to that file (*Col 5, lines 11-16 & Col 2, lines 44-51*);

action determination code operable, if the count value determined by the statistical log interface code exceeds a predetermined threshold (Col 6, lines 15-28) but he doesn't explicitly disclose a weighting table identifying, for each value of the predetermined attributes, a weighting indicating the likelihood that a file having that value of predetermined attributes will be malware and to reference the weighting table to determine the weighting to be associated with the file in case the count value exceeds the threshold and take actions based on that weight.

However Smithson discloses a method for computer virus detection where he discloses a method for detecting computer viruses based on some predetermined criteria like the count of the file (See Abstract) where he teaches using a weighting table identifying, for each value of predetermined attributes (*Col 4, lines 50- 62 & Col 9, lines 21-27*), a weighting indicating the likelihood that a file having that value of said one or more predetermined attributes will be malware (*Col 4, lines 5-20*), based on the value of said one or more predetermined attributes associated with that file in the statistical log (*Col 4, lines 25-40 & Col 6, lines 35-43)*; and performing a predetermined actions dependent on the weighting determined by determination code (*Col 6, lines 34-44* & *Col 8, lines 13-31*). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Chess system with the teachings of Smithson to base actions based on a weighting tables for the files. One would be motivated to do so in order to enable the system to detect unknown viruses, because using such technique is not looking for an individual virus or pattern of execution of a virus, it is able to more readily detect previously unknown viruses by the effect that they have on the activity of the computer system as a whole (*Smithson: Col 2, lines 10-15*).

Regarding claims 2, 15 & 28: The computer program product as combined in claim 1, further discloses the computer program product, wherein said one or more predetermined attributes comprise an indication of the file type of the file (*Chess: Col 4, lines 24-34*).

Regarding claims 7, 20 & 33: The computer program product as combined in claim 1, discloses the computer program product, wherein if the weighting indicates that the file is to be treated with caution, said action performing code is operable to perform the steps of: associating a warning message with the file for reference by a person receiving that file (*Chess: Col 5, lines 39-46 / "questionable" status*); and (ii) generating for access by an administrator a notification identifying the file (*Chess: Col 6, lines 54-65*).

Regarding claims 8, 21 & 34: The computer program product as combined in claim 1, further discloses if the weighting indicates that the file is safe, said action performing code is operable to generate for access by an administrator a notification identifying the file (*Smithson: Col 8, lines 54-60 / notification will be sent to administrator*).

Regarding claims 9, 22 & 35: The computer program product as combined in claim 1, further discloses the computer program product, wherein if it is determined that a file sent to the computer is not currently entered in the statistical log (*Chess: 301 of FIG. 3A*), the logging code is further operable to create an entry in the statistical log for the file (*Chess: Col 5, lines11-20*), in which the value of said one or more predetermined attributes relating to the file are stored, and in which the count value is initialised (*Chess: Col 5, lines 20-29 & Col 5, lines 1-5*).

Regarding claims 10, 23 & 36: The computer program product as combined in claim 1, further discloses the computer program product, wherein upon receipt of a file, the statistical log interface code is operable to cause the count value within the relevant entry of the statistical log to be incremented to account for the current occurrence of the file (*Chess: Col 4, line 62 through Col 5, line 5 & Col 2, lines 44-51*).

Regarding claims 11, 24 & 37: The computer program product as combined in claim 1, further discloses the computer arranged to review files included in e-mail communications (*Smithson: Col 3, lines 26-33*), and each entry in the statistical log is further arranged to identify, for each sender of that file, the number of times that that sender has sent the file in addition to the count value indicating the total number of times that the file has been sent (*Smithson: Col 4, lines 25-40*).

Regarding claims 12, 25 & 38: A computer program product as claimed in claim 11, further discloses upon receipt of a file, the statistical log interface code is operable to cause the count value within the relevant entry of the statistical log to be incremented to account for the current occurrence of the file (*Chess: Col 3, lines 17-23*), and the number by which the count value is incremented is dependent on the number of times that the sender of the current occurrence of the file has previously sent that file (*Chess: Col 5, lines 11-28*).

1. Claims 3-6, 13, 16-19, 26, 29-32 & 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chess et al. US (6,711,583) in view of Smithson et al. US (6,886,099) as applied to claims 1, 14 & 27 above, and further in view of Templeton US (6,401,210).

Regarding claims 3, 16 & 29: The computer program product as combined in claim 1 further discloses if the weighting indicates that the file is probably malware, said action performing code is operable to perform the steps of: Notifying the user of the file (Col 6, lines 51-62) but the combination doesn't disclose encrypting the file such that only an administrator can decrypt that file. However Templeton discloses a method for managing virus infected files (See Abstract) where he teaches detecting a virus in a file encrypting the file in such a way that only the administrator (system operator) can decrypt that file (*Col 4, line*

64 through Col 5, line 5 & Col 3, lines 23-27). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to combine the teachings of Chess and Smithson with the teachings of Templeton to encrypt the file after detecting a virus present in the file in was that only the administrator can decrypt the file. One would be motivated to do so in order enable the system to safely store files that have a high probability of being infected and prevent the user from opening the files and spreading the virus to another files or computers while being able to reproduce the original file for further analysis or cleaning at later time (*Col 1, lines 44-54*).

Regarding claims 4, 17 & 30: The system as combine in claim 3 is further operable to associate a message with the file for reference by a person receiving that file, the message identifying that the file has been encrypted (*Col 3, lines 61-64 & Col 4, lines 29-40*).

Regarding claims 5, 18 & 31: A computer program product as claimed in claim 1, wherein if the weighting indicates that the file is possibly malware, said action performing code is operable to perform the steps of:

Notifying the user of the file (Col 6, lines 51-62) but the combination doesn't disclose encrypting the file such that only an administrator and the originator of the file can decrypt that file. However Templeton discloses a method for managing virus infected files (See Abstract) where he teaches upon detecting a virus in a file encrypting the file (*Templeton: Col 4, line 64 through Col 5, line 5*) in such a way that only the system operator or the owner can decrypt that file (*Templeton: Col 3, lines 23-27 & Col 3, lines 50-55*). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to combine the teachings of Chess and Smithson with the teachings of Templeton to encrypt the file after detecting a virus present in the file in was that only the administrator or the owner can decrypt the file. One would be motivated to do so in order enable the system to safely store files that have a high probability of being infected and prevent the recipients from opening the files and spreading the virus to another files or computers while being able to reproduce the original file for further analysis or cleaning at later time (*Col 1, lines 44-54*).

Regarding claims 6, 19 & 32: A computer program product as claimed in claim 5, wherein the action performing code is further operable to associate a message with the file for reference by a person receiving that file, the message identifying that the file has been encrypted (*Templeton: Col 3, lines 61-64 & Col 4, lines 29-40)*.

Regarding claims 13, 26 & 39: The computer program product as combined in claim 1, further discloses the computer program product as claimed in claim 1, wherein if said action performing code is arranged, dependent on the weighting (*Smithson: Col 5, line 65 through Col 6, line 3*), to quarantine the file or delete it but the combination doesn't disclose encrypting the file and an automated decryption code operable, if the file is subsequently determined to be safe, to perform the steps of: locating all encrypted occurrences of that file on a file system; and decrypting each said occurrence. However Templeton discloses a method for managing virus infected files (*See Abstract*) where he teaches after determining that a file has been infected (*Templeton: Col 4, lines 41-45*), encrypting that file for later time (*Templeton: Col 4, lines 64-67*) and when a determination is made that the file is safe to locate the file and decrypt each occurrence of that file (*Templeton: Col 5, lines 16-31*). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify the system to include locating and decrypting files that have been determined to be safe. One would be motivated to do so to enable the user to view and use files that have been analyzed and determined to be free from viruses.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firas Alomari whose telephone number is (571) 272-7963. The examiner can normally be reached on M-F from 8:30 am - 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ SHEIKH can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Firas Alomari
Examiner
Art Unit 2136

FA

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100